



**7710-12**

## **POSTAL SERVICE**

### **Privacy Act of 1974; System of Records**

**AGENCY:** Postal Service™.

**ACTION:** Notice of a modified system of records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the United States Postal Service® (Postal Service) is revising the notice for Privacy Act System of Records USPS 910.000, Identity and Document Verification Services.

**DATES:** These revisions will become effective without further notice on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER] unless comments received on or before that date result in a contrary determination.

**ADDRESSES:** Comments may be mailed or delivered to the Privacy and Records Management Office, United States Postal Service, 475 L'Enfant Plaza SW, Room 1P830, Washington, DC 20260-1101. Copies of all written comments will be available at this address for public inspection and photocopying between 8 a.m. and 4 p.m., Monday through Friday.

**FOR FURTHER INFORMATION CONTACT:** Janine Castorina, Chief Privacy and Records Management Officer, Privacy and Records Management Office, 202-268-3069 or [privacy@usps.gov](mailto:privacy@usps.gov).

**SUPPLEMENTARY INFORMATION:** This notice is in accordance with the Privacy Act requirement that agencies publish their systems of records in the Federal Register when there is a revision, change, or addition, or when the agency establishes a new system of records. As detailed below, the Postal Service has determined that USPS 910.000, Identity and Document Verification Services should be revised to modify Categories of

Individuals Covered by the System, Categories of Records in the System, Purpose(s), and Retention and Disposal.

The changes are being made to:

- a. Support the new Address Matching Database, which will be used to identify, prevent and mitigate fraudulent activity within the Change of Address and Hold Mail processes.
- b. Allow for the scanning of Government issued IDs at retail locations for the purposes of verifying identity for customers who need postal products and services.
- c. To enhance the Postal Service's existing remote identity proofing with a Phone Validation and One-Time Passcode solution.

The new Address Matching Database is being implemented to identify, prevent and mitigate fraudulent activity within the Change of Address and Hold Mail processes. The Postal Service is establishing a dataflow between existing customer systems and the Address Matching Database. This dataflow will allow the Address Matching Database to: confirm if there is an address match when a new Hold Mail request is submitted; confirm the presence of a Change of Address request when a Hold Mail request is submitted during a 30 day time frame; and confirm the presence of a Hold Mail request when a Change of Address request is submitted during a 30 day time frame. The Address Matching Database will also send confirmation notifications to customers who submit a Hold Mail request.

The capability to scan Government issued IDs is being implemented to verify identity when requesting government-issued ID to reduce fraudulent cases surrounding USPS programs and the disposition of certain customer mail services. This will provide the Postal Service the ability to capture and store information provided in the 2-

Dimensional barcode on government issued photo IDs (e.g. State-issued driver or non-driver licenses and military IDs).

The Phone Validation and One-Time Passcode solution is being implemented to enhance the Postal Service's existing remote identity proofing solution and to detect, to the best extent possible, the presentation of fraudulent identities by a malicious user. The Postal Service's objective in implementing the Phone Validation and One-Time Passcode solution is to ensure the user is who they claim to be to a stated level of certitude. The validation and verification of the minimum attributes necessary is used to accomplish identity proofing.

Pursuant to 5 U.S.C. 552a(e)(11), interested persons are invited to submit written data, views, or arguments on this proposal. A report of the proposed revisions has been sent to Congress and to the Office of Management and Budget for their evaluations. The Postal Service does not expect these amended systems of records to have any adverse effect on individual privacy rights. The notice for USPS 910.000, Identity and Document Verification Services, provided below in its entirety, is as follows:

**SYSTEM NAME AND NUMBER:**

USPS 910.000, Identity and Document Verification Services.

**SYSTEM CLASSIFICATION:**

None.

**SYSTEM LOCATION:**

USPS Marketing, Headquarters; Integrated Business Solutions Services Centers; and contractor sites.

**SYSTEM MANAGER(S)**

Chief Information Officer and Executive Vice President, United States Postal Service,  
475 L'Enfant Plaza SW, Washington, DC 20260-1500; (202) 268-6900

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

39 U.S.C. 401, 403, 404, and 411.

**PURPOSE(S) OF THE SYSTEM:**

1. To provide services related to identity and document verification services.
2. To issue and manage public key certificates, user registration, email addresses, and/or electronic postmarks.
3. To provide secure mailing services.
4. To protect business and personal communications.
5. To enhance personal identity and privacy protections.
6. To improve the customer experience and facilitate the provision of accurate and reliable delivery information.
7. To identify, prevent, or mitigate the effects of fraudulent transactions.
8. To support other Federal Government Agencies by providing authorized services.

9. To ensure the quality and integrity of records.
10. To enhance the customer experience by improving the security of Change of Address (COA) and Hold Mail processes.
11. To protect USPS customers from becoming potential victims of mail fraud and identity theft.
12. To identify and mitigate potential fraud in the COA and Hold Mail processes.
13. To verify a customer's identity when applying for COA and Hold Mail services.
14. To provide an audit trail for COA and Hold Mail requests (linked to the identity of the submitter).
15. To enhance remote identity proofing with a Phone Validation and One-Time Passcode solution.

#### **CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

1. Customers who apply for identity and document verification services.
2. Customers who may require identity verification for Postal products and services.

#### **CATEGORIES OF RECORDS IN THE SYSTEM:**

1. *Customer information:* Name, address, customer ID(s), telephone number, text message number and carrier, mail and email address, date of birth, place of birth, company name, title, role, and employment status.
2. *Customer preference information:* Preferred means of contact.
3. *Authorized User Information:* Names and contact information of users who are authorized to have access to data.
4. *Verification and payment information:* Credit and/or debit card information or other account number, government issued ID type and number, verification question and answer, and payment confirmation code. (*Note:* Social Security

Number and credit and/or debit card information are collected, but not stored, in order to verify ID.)

5. *Biometric information:* Fingerprint, photograph, height, weight, and iris scans.  
(Note: Information may be collected, secured, and returned to customer or third parties at the direction of the customer, but not stored.)
6. *Digital certificate information:* Customer's public key(s), certificate serial numbers, distinguished name, effective dates of authorized certificates, certificate algorithm, date of revocation or expiration of certificate, and USPS-authorized digital signature.
7. *Online user information:* Device identification.
8. *Transaction information:* Clerk signature; transaction type, date and time, location, source of transaction; product use and inquiries; Change of Address (COA) and Hold Mail transactional data.
9. *Electronic information:* Information related to encrypted or hashed documents.
10. *Recipient information:* Electronic signature ID, electronic signature image, electronic signature expiration date, and timestamp.

#### **RECORD SOURCE CATEGORIES:**

Customers.

#### **ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:**

Standard routine uses 1. through 7., 10., and 11. apply.

#### **POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:**

By customer name, customer ID(s), distinguished name, certificate serial number, receipt number, and transaction date.

#### **POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:**

1. Records related to Pending Public Key Certificate Application Files are added as received to an electronic database, moved to the authorized certificate file when they are updated with the required data, and records not updated within 90 days from the date of receipt are destroyed.
2. Records related to the Public Key Certificate Directory are retained in an electronic database, are consistently updated, and records are destroyed as they are superseded or deleted.
3. Records related to the Authorized Public Key Certificate Master File are retained in an electronic database for the life of the authorized certificate.
4. When the certificate is revoked, it is moved to the certificate revocation file.
5. The Public Key Certificate Revocation List is cut off at the end of each calendar year and records are retained 30 years from the date of cutoff. Records may be retained longer with customer consent or request.
6. Other records in this system are retained 7 years, unless retained longer by request of the customer.
7. Records related to electronic signatures are retained in an electronic database for 3 years.
8. Other categories of records are retained for a period of up to 30 days.
9. Driver's License data will be retained for 5 years.
10. COA and Hold Mail transactional data will be retained for 5 years.

Records existing on paper are destroyed by burning, pulping, or shredding. Records existing on computer storage media are destroyed according to the applicable USPS media sanitization practice.

#### **ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:**

Paper records, computers, and computer storage media are located in controlled-access

areas under supervision of program personnel. Access to these areas is limited to authorized personnel, who must be identified with a badge.

Access to records is limited to individuals whose official duties require such access.

Contractors and licensees are subject to contract controls and unannounced on-site audits and inspections.

Computers are protected by mechanical locks, card key systems, or other physical access control methods. The use of computer systems is regulated with installed security software, computer logon identifications, and operating system controls including access controls, terminal and transaction logging, and file management software.

Key pairs are protected against cryptanalysis by encrypting the private key and by using a shared secret algorithm to protect the encryption key, and the certificate authority key is stored in a separate, tamperproof, hardware device. Activities are audited, and archived information is protected from corruption, deletion, and modification.

For authentication services and electronic postmark, electronic data is transmitted via secure socket layer (SSL) encryption to a secured data center. Computer media are stored within a secured, locked room within the facility. Access to the database is limited to the system administrator, database administrator, and designated support personnel. Paper forms are stored within a secured area within locked cabinets.

#### **RECORD ACCESS PROCEDURES:**

Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.6.

#### **CONTESTING RECORD PROCEDURES:**

See [Notification Procedures](#) below and [Record Access Procedures](#) above.



**NOTIFICATION PROCEDURES:**

Customers wanting to know if other information about them is maintained in this system of records must address inquiries in writing to the system manager, and include their name and address.

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:**

None.

**HISTORY:**

December 22, 2017, [82 FR 60776](#); August 29, 2014, [79 FR 51627](#); October 24, 2011, [76 FR 65756](#); April 29, 2005, [70 FR 22516](#).

\* \* \* \* \*

Brittany M. Johnson

Attorney, Federal Compliance.